REMARKS

The Examiner is thanked for the performance of a thorough search. By this amendment, Claims 9-12 have been cancelled and Claims 1, 3, 5, 7, 13, 15, 17 and 18 have been amended. Hence, Claims 1-8 and 13-19 are pending in the application. It is respectfully submitted that none of the claim amendments add any new matter to this application. All issues raised in the Office Action mailed June 25, 1999 are addressed hereinafter.

REJECTION OF CLAIMS 1, 2, 5, 6, 13 AND 14 UNDER 35 U.S.C. §103(a)

Claims 1, 2, 5, 6, 13 and 14 were rejected under 35 U.S.C. §103(a) as being unpatentable over *Gillon et al.,* (*"Gillon"*) U.S. Patent No. 5,838,927 in view of *Elgamal et al.*, (*"Elgamal"*) U.S. Patent No. 5,657,390 and *Shaffer et al.*, (*"Shaffer"*) U.S. Patent No. 5,784,461. It is respectfully submitted that Claims 1, 2, 5, 6, 13 and 14, as amended, are patentable over *Gillon* in view of *Elgamal* and *Shaffer* for at least the reasons set forth hereinafter.

CLAIM 1

Claim 1 recites a method "for providing communication protocol-independent security for data transmitted between a first process, executing on a first network node, and a second process, executing on a second network node, where in the first network node and the second network node each support at least one common communication protocol." Claim 1 requires the steps of:

"a) establishing a communication channel between the first network node and the second network node;

b) establishing a first stream between the first process and the communication channel;

c) establishing a second stream between the second process and the communication channel;

d) in response to the data being written to the first stream, encrypting the data to generate encrypted data, the encrypting of the data being performed independent of any communication protocols used to transport the encrypted data from the first network node to the second network node;

e) causing the encrypted data to be transmitted from the first network node to the second network node according to the at least one communication protocol supported by the first and second network nodes; and

f) in response to the encrypted data being read from the second stream, decrypting the encrypted data to recover decrypted data which is identical to the data on the first network node before the data was written to the first stream, the decrypting of the encrypted data being performed independent of any communication protocols used to transport the encrypted data from the first network node to the second network node."

The invention recited in Claim 1 addresses the problem of how to provide layer-independent secure communications in a multi-layered communications network. Claim 1, as amended, requires that data to be transported from the first network node to the second network node be encrypted and decrypted in response to the data being written to and read from the first and second streams, respectively. As a result, all data transported between the first and second network nodes is always encrypted during transport, regardless of whether any additional external encryption has been performed. This approach removes the burden of encrypting and decrypting the data from the first and second processes. Furthermore, there is no need for a customized communications protocol to handle encryption and decryption of data. Rather, as recited in amended Claim 1, the encryption is performed "in response to the data being written to the first stream" and the decryption is performed "in response to the encrypted data being read from the second stream."

It is respectfully submitted that *Gillon, Elgamal* and *Shaffer*, do not teach or suggest, alone or in combination, the method recited in Claim 1. *Gillon* describes an approach for compressing a continuous, indistinct data stream that involves examining a data stream to determine whether the data stream is compressible. If the data stream is compressible, then the data stream is attached to a compression stream and compression is performed to generate a compressed data stream that is transmitted continuously as it is generated. However, *Gillon* does not describe how the encryption of a data stream is performed and in particular, does not teach or suggest encrypting and decrypting data as the data is written to and read from first and second streams, respectively, as is required by amended Claim 1.

Elgamal describes an approach for encrypting and decrypting information transferred over a network between a client application and a server application. A sockets application program interface is bound to a security protocol which is layered between an application layer and a transport layer. The security protocol is implemented the application layer and the transport layer and not when data is written to and read from streams, as is required by amended Claim 1.

Shaffer describes an approach for controlling access to images and image related services by encrypting data and service requests exchange between a fulfillment center and a customer. In *Shaffer* data and service requests are encrypted before being transmitted on a communications link. Thus, the customer site is responsible for encrypting the data to ensure the safety of the data during transport to the fulfillment center.

For these reasons, it is respectfully submitted that *Gillon*, *Elgamal* and *Shaffer* do not teach or suggest encrypting and decrypting data in response to the data being written to and read from first and second streams, respectively, as is required by amended Claim 1.

CLAIMS 2, 5, 6, 13 AND 14

Claims 5 and 13 are directed to a computer-readable medium and a computer data signal, respectively, that recite similar limitations to Claim 1. Therefore, it is respectfully submitted that Claims 5 and 13 are patentable over *Gillon* in view of *Elgamal* and *Shaffer* for the reasons stated herein with respect to Claim 1.

Claims 2, 6 and 14 depend from Claims 1, 5 and 13 and include all the limitations of Claims 1, 5 and 13. Therefore, it is respectfully submitted that Claims 2, 6 and 14 are patentable over *Gillon* in view of *Elgamal* and *Shaffer* for the reasons stated herein in support of Claims 1, 5 and 13.

For these reasons, the reconsideration and withdrawal of the rejection of Claims 1, 2, 5, 6, 13 and 14 under 35 U.S.C. §103(a) as being unpatentable over *Gillon* in view of *Elgamal* and *Shaffer* is respectfully requested.

REJECTION OF CLAIMS 3, 4, 7, 8, 15 AND 16 UNDER 35 U.S.C. §103(a)

Claims 3, 4, 7, 8, 15 and 16 were rejected under 35 U.S.C. §103(a) as being unpatentable over *Gillon* in view of *Elgamal* and *Shaffer* and further in view of *van Hoff et al.*, ("*van Hoff*") U.S. Patent No. 5,761,421. It is respectfully submitted that Claims 3, 4, 7, 8, 15 and 16 are patentable over *Gillon* in view of *Elgamal* and *Shaffer* and further in view of *van Hoff* for at least the following reasons.

Van Hoff describes an approach for providing secure peer-to-peer communication between downloaded programs. The approach allows two programs obtained from the same security domain and executing on two different client computers to communicate securely. *Van Hoff* does not each or suggest the step of "in response to the data being written to the first stream, encrypting the data to generate encrypted data, the encrypting of the data being performed independent of any communication protocols used to transport the encrypted data from the first network node to the second network node" or the step of "in response to the encrypted data being read from the second stream, decrypting the encrypted data to recover decrypted data which is identical to the data on the first network node before the data was written to the first stream, the decrypting of the encrypted data being performed independent of any communication protocols used to transport the encrypted data from the first network node to the second network node" as are required by Claims 3, 4, 7, 8, 15 and 16. There is no mention in *van Hoff* of encrypting and decrypting data in response to writing and reading the data to and from a stream, respectively, as is required by Claims 3, 4, 7, 8, 15 and 16.

Therefore, since as previously described, *Gillon*, *Elgamal* and *Shaffer*, alone or in combination, do not teach or suggest these steps, it is respectfully submitted that Claims 3, 4, 7, 8, 15 and 16 are patentable over *Gillon* in view of *Elgamal* and *Shaffer* and further in view of *van Hoff*. Accordingly, the reconsideration and withdrawal of the rejection of Claims 3, 4, 7, 8, 15 and 17 under 35 U.S.C. §103(a) as being unpatentable over *Gillon* in view of *Elgamal* and *Shaffer* and further in view of *van Hoff* is respectfully requested.

REJECTION OF CLAIMS 9 AND 10 UNDER 35 U.S.C. §103(a)

Claims 9 and 10 were rejected under 35 U.S.C. §103(a) as being unpatentable over *Elgamal* in view of *Gillon* and *Shaffer*. It is respectfully submitted that this rejection is now moot in view of the cancellation of Claims 9 and 10.

REJECTION OF CLAIMS 11 AND 12 UNDER 35 U.S.C. §103(a)

Claims 11 and 12 are rejected under 35 U.S.C. §103(a) as being unpatentable over *Elgamal* in view of *Gillon* and *Shaffer* and further in view of *van Hoff*. It is respectfully submitted that this rejection is not moot in view of the cancellation of Claims 11 and 12.

REJECTION OF CLAIM 17 UNDER 35 U.S.C. §103(a)

Claim 17 has been rejected under 35 U.S.C. §103(a) as being unpatentable over *Gillon* in view of *Elgamal* and *Shaffer*. It is respectfully submitted that Claim 17, as amended, is patentable over *Gillon* in view of *Elgamal* and *Shaffer* for at least the reasons provided hereinafter. Claim 17 recites a method for providing communication protocol-independent security for data transmitted by a process executing on a network node. The method recited in amended Claim 17 requires the steps of:

> "a) establishing a stream between the process and a communications channel; and
> b) in response to the data being written to the stream, encrypting the data to generate encrypted data, the encrypting of the data being performed independent of any communications protocol used to transport the encrypted data on the communications channel."

Claim 17 addresses the problem of how to provide communication protocol-independent security for data transmitted by a process executing on a network node. Claim 17 solves this problem by encrypting data in response to the data being written to the stream. This relieves the process that transmits the data from the responsibility for encrypting the data. According to the approach recited in amended Claim17, all data written to the stream is automatically encrypted and protected during transport over the communications channel.

As previously described herein with respect to Claim 1, *Gillon, Elgamal* and *Shaffer*, do not teach or suggest, alone or in combination, encrypting data in response to the data being written to a stream. Therefore, it is respectfully submitted that Claim 17 is patentable over *Gillon* in view of *Elgamal* and *Shaffer*. Accordingly, the reconsideration and withdrawal of the rejection of Claim 17 under 35 U.S.C. §103(a) as being unpatentable over *Gillon* in view of *Elgamal* and *Shaffer* is respectfully requested.

REJECTION OF CLAIMS 18 AND 19 UNDER 35 U.S.C. §103(a)

Claims 18 and 19 were rejected under 35 U.S.C. §103(a) as being unpatentable over *Gillon* in view of *Elgamal* and *Shaffer* and further in view of *van Hoff*. It is respectfully submitted that Claims 18 and 19 are not unpatentable over *Gillon* in view of *Elgamal* and *Shaffer* and further in view of *van Hoff* for at least the reasons provided hereinafter.

Claims 18 and 19 depend on Claim 17 and include all the limitations of Claim 17. Specifically, Claims 18 and 19 require the step of "in response to the data being written to the stream, encrypting the data to generate encrypted data, the encrypting of the data being performed independent of any communications protocol used to transport the encrypted data on the communications channel." As previously described with respect to Claims 1, 3, 4, 7, 8, 15 and 16, *Gillon*, *Elgamal*, *Shaffer* and *van Hoff* do not teach or suggest, alone or in combination, encrypting data in response to writing the data to a stream, as is required by Claims 18 and 19. Therefore, it is respectfully submitted that Claims 18 and 19, as amended, are patentable over *Gillon* in view of *Elgamal* and *Shaffer* and further in view of *van Hoff.*

Accordingly, the reconsideration and withdrawal of the rejection of Claims 18 and 19 under 35 U.S.C. 103(a) as being unpatentable over *Gillon* in view of *Elgamal* and *Shafer* and further in view of *van Hoff* is respectfully requested.

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a notice of allowance is respectfully requested. The Examiner is invited to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

If there are any additional charges, please charge them to our Deposit Account No. 50-0385.

Respectfully submitted,
McDERMOTT, WILL & EMERY

Brian D. Hickman
Reg. No. 35,894

600 13th Street, N.W.
Washington, DC 20005-3096
(408) 271-2300 EAB:ccf
Date: November 19, 1999
Facsimile: (408) 271-2310

CERTIFICATE OF MAILING
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, DC 20231

on 11/19/99 by